Amendments to the Specification

On page 4, lines 4-21, please replace the existing paragraph with the following substitute paragraph:

A crypto key is maintained on a secure key repository, such as on an IMD, and is used to preencrypt sensitive information, including any PHI, prior to storage on the IMD. The crypto key can either be pre-programmed and persistently stored on the IMD, or can be dynamically generated on the IMD, programmer or dedicated repeater. The crypto key is retrieved by the programmer or repeater from the source of the crypto key based on the form of the key and the type of device maintaining the crypto key, such as described in commonly-assigned U.S. Patent application ~~Serial No. _____~~ Serial No. 10/800,806, entitled "System And Method For Securely Authenticating A Data Exchange Session With An Implantable Medical Device," ~~Attorney Docket No. 020.0328.US.UTL,~~ filed March 15, 2004, pending, the disclosure of which is incorporated by reference. The sensitive information is then encrypted by the programmer or repeater using the crypto key and is stored onto the IMD. Since the sensitive information is in an encrypted form, the encrypted sensitive information can be sent through secure, short range telemetry or using, for example, long range telemetry, such as RF telemetry, or other unsecured data interfaces. Subsequently, the encrypted sensitive information is retrieved from the IMD and is decrypted using the crypto key.

On page 8, lines 13-29, please replace the existing paragraphs with the following substitute paragraphs:

In a further embodiment, the IMD 103 includes a telemetry interlock that limits communication between the IMD 103 and an external device. Patient/clinician authentication is secured through release of the telemetry interlock, which can be used in conjunction with secure crypto key 122 retrieval. The telemetry interlock is released when the external device transmits an

ENABLE command to the IMD 103 via short range telemetry, such as described in commonly-assigned U.S. Patent ~~application Serial No. 10/601,763, filed June 23, 2003, pending~~ No. 7,155,290, issued December 26, 2006, the disclosure of which is incorporated by reference.

In a further embodiment, the IMD 103 can verify the integrity of messages received from a programmer 123, repeater 124 or other wireless computing device 125 and, alternatively, a programmer 123, repeater 124 or other wireless computing device 125 can verify the integrity of messages received from IMD 103, both using a symmetric encryption algorithm or one-way hash algorithm, such as described in commonly-assigned U.S. Patent ~~application Serial No. _____, entitled "Cryptographic Authentication for Telemetry With An Implantable Medical Device," Attorney Docket No. 0279.718US1, filed March 15, 2004, pending~~ No. 7,228,182, issued June 5, 2007, the disclosure of which is incorporated by reference.

On page 10, lines 12-30, please replace the existing paragraph with the following substitute paragraph:

Authentication 126 involves an affirmative interaction between a patient and a clinician during which the clinician informs the patient, either directly or by implication, and secures authorization to access the patient information, including any static data constituting sensitive information, maintained in the IMD 103 and, if necessary, to interrogate and reprogram the IMD 103. Authentication 126 ensures that a clinician does not accidentally start a data exchange session with the wrong patient or without a patient's knowledge. Authentication 126 also provides an opportunity to securely obtain the crypto key 122 uniquely associated with the IMD 103. During authentication 126, the IMD 103 interfaces with an external source, such as a programmer 123, repeater 124 or other wireless computing device 125, to either receive or share the crypto key 122 assigned to the IMD 103, such as described in commonly-assigned U.S. Patent application ~~Serial No. _____~~ Serial No. 10/800,806, entitled "System And Method For

Securely Authenticating A Data Exchange Session With An Implantable Medical Device," ~~Attorney Docket No. 020.0328.US.UTL,~~ filed March 15, 2004, pending, the disclosure of which is incorporated by reference. In one embodiment, the external source retrieves the crypto key 122 from the IMD 103 using secure, short range telemetry, such as inductive telemetry, as further described below with reference to FIGURE 4.

On page 11, lines 1-24, please replace the existing paragraph with the following substitute paragraph:

Authentication 126 must be completed prior to protected data storage and retrieval 129. Upon completing authentication 126, sensitive information 127 (SI), particularly PHI, is received into the external device from a patient or clinician and part or all of the sensitive information 127 is preencrypted by a programmer 123 or repeater 124 using the crypto key 122. Preencryption places the burden of active encryption and decryption on the external device, rather than on the IMD 103, for sensitive information stored but not actually used by the IMD 103. The preencrypted sensitive information 128 is then sent to the IMD 103. The preencrypted sensitive information 128 can be sent through secure, short range telemetry or using, for example, long range telemetry, such as RF telemetry, or other unsecured data interfaces. Preencryption allows sensitive information to be securely transmitted over an RF or other long range wireless link in compliance with applicable patient health information privacy laws and regulations. If the sensitive information needs to be retrieved, the external source obtains the crypto key 122, if necessary, through authentication 126 and retrieves the encrypted information 128 from the IMD 103 for subsequent decryption using the crypto key 122. In one embodiment, the sensitive information 127, including any PHI, is encrypted using a standard encryption protocol, such as the Advanced Encryption Standard protocol (AES). Other authentication and encryption techniques and protocols, as well as other functions relating to the use of the crypto key 122 are possible, including the authentication and encryption

techniques and protocols described in commonly-assigned U.S. Patent ~~application Serial No. 10/601,763, filed June 23, 2003, pending~~ No. 7,155,290, issued December 26, 2006, the disclosure of which is incorporated by reference.

On page 17, lines 18-24, please replace the existing paragraph with the following substitute paragraph:

In further embodiment, the crypto key 122 is retrieved using a patient designator, through a secure lookup, using a physical token, and with a repeater to provide patent/clinician authentication, such as described in commonly-assigned U.S. Patent application ~~Serial No. _____~~ Serial No. 10/800,806, entitled "System And Method For Securely Authenticating A Data Exchange Session With An Implantable Medical Device," ~~Attorney Docket No. 020.0328.US.UTL,~~ filed March 15, 2004, pending, the disclosure of which is incorporated by reference.